WABUSK DATA SOLUTIONS

"Committed to Indigenous data sovereignty and respectful, reciprocal relationships."

www.wabuskdata.ca
info@wabuskdata.ca
Operating across Turtle Island

Submission to the Office of the Privacy Commissioner of Canada (OPC) on the Development of the Children's Privacy Code

Date: July 31, 2025

To: The Honourable Office of the Privacy Commissioner of Canada

We extend our gratitude for the opportunity to provide input on the development of the forthcoming Children's Privacy Code, and we recognize the leadership role the OPC plays in shaping privacy culture globally and protections under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) here in Canada. While we acknowledge that the OPC's mandate is bound by the current federal legislative framework, we respectfully assert that your role as Canada's national privacy oversight body also carries a moral and social responsibility to look beyond existing statutes. In doing so, the OPC must ensure that the systems it upholds do not unintentionally perpetuate colonial harms or reinforce inequities that fail to serve all children—especially Indigenous children.

The Children's Privacy Code is a critical step toward protecting children in the digital age. But if it is to be effective, equitable, and rights-based, it must explicitly address the intersectional, systemic, and culturally specific risks that Indigenous children and youth face in both online and offline environments. Below, we offer feedback and recommendations based on our work in Indigenous data governance, child and family wellbeing, and digital rights advocacy.

Application of the Code

We urge the OPC to adopt a broader and more inclusive approach to accountability under the Code. While there is growing momentum to hold the private sector to high standards, public institutions often escape equivalent scrutiny, even as they routinely collect and manage some of the most sensitive data about children — including health, education, justice, and child welfare information.

These public systems frequently lack transparency, meaningful consent mechanisms, and culturally appropriate oversight — especially when it comes to Indigenous children. Yet they are often the most powerful sources of surveillance, control, and harm in these communities. The digital rights conversation must move beyond its narrow focus on private sector advertising and recognize the deep-rooted data colonialism embedded in child-serving institutions.

If we are truly committed to protecting Indigenous children, public systems must undergo deep interrogation and transformation.

We offer the following questions for your consideration:

- ➔ How will this Code intersect with privacy laws and data governance frameworks across sectors?
- ➔ How will it support harmonization with Indigenous-led laws, protocols, and community-defined standards for child wellbeing and data stewardship.

A Call for Ethical Accountability

We are concerned that current compliance frameworks — such as privacy impact assessments (PIAs) and risk assessments — are often used as checkboxes to avoid deeper conversations about equity and sovereignty. In our experience, these tools rarely engage with Indigenous data governance principles unless purposely built from that lens.

What is needed is not just legal sufficiency but ethical and relational accountability. This means being willing to face the long-term and structural impacts of how information about Indigenous children is gathered, stored, shared, and acted upon.

Online Risks to Indigenous Children

The risks faced by Indigenous children in digital environments are distinct, deeply rooted in history, and compounded by systemic neglect. These risks must be explicitly named and addressed in the Code to avoid further marginalization.

Artificial intelligence (AI) platforms used to explore Indigenous language, ceremony, or identity often produce distorted or inaccurate results, reinforcing patterns of digital colonialism and contributing to the ongoing misrepresentation of Indigenous cultures. This is a particular concern for children and youth who are looking to the digital world for connection and information about their culture. These harms are compounded by the rise of photo manipulation and deepfake technologies, which pose serious risks to all children but especially to Indigenous girls, who already face disproportionate rates of violence, oversexualization, and trafficking. In parallel, the surveillance of Indigenous activists for the purpose of criminalization when we are seeing a growing number of youth engaged in political organizing, land defense, or cultural resurgence must be recognized and addressed as a form of systemic overreach, and such monitoring must be explicitly prohibited in any framework aiming to uphold the rights of Indigenous children.

While we understand the intent behind the concept of “no-go zones,” we have concerns about how such restrictions can be manipulated or bypassed through technical loopholes and regulatory workarounds. Rather than relying solely on exclusion zones, we advocate for approaches rooted in informed decision-making, transparent accountability, and clearly defined boundaries. That said, there must be strong and specific protections in place. The Code must establish safeguards for the cultural, spiritual, and political data that Indigenous youth share or engage with online, and it must recognize that consent for community-based data related to Indigenous Peoples requires collective authorization—not just individual permission.

Consent: Capacity & Accessibility

The Code must strike a careful balance between legal thresholds and developmental appropriateness, recognizing that consent is not a one-size-fits-all concept. We encourage the OPC to move beyond rigid age-based models and toward contextual assessments of capacity that are culturally grounded, rights-affirming, and aligned with principles of child development.

We also urge the OPC to account for the realities of children who do not live in traditional family structures. Indigenous children are disproportionately represented in the child welfare system and among unhoused populations. Many live in group homes or temporary care arrangements without stable access to a reliable caregiver. A consent model that assumes a consistent caregiver risks excluding the most vulnerable from essential digital environments.

In line with international child rights principles, we strongly support the use of opt-in consent mechanisms over default or passive data collection. Children should never be automatically opted into data processing. The most privacy-protective settings should be applied by default, particularly for younger users and those navigating high-risk contexts. Consent must not be treated as a checkbox—it must be a meaningful process that empowers children to understand what they are agreeing to before they give permission.

To that end, the Code should require that consent mechanisms are accessible, youth-friendly, and culturally appropriate. This may involve offering information in audio or visual formats, using icons, illustrations, or colour-coded systems in place of dense legal text. Legal jargon creates barriers to understanding and undermines children's ability to make informed decisions. Privacy information should not only inform—it should educate and empower.

With these comments in mind we'd pose the following questions for the OPC to consider:

- ➔ How will platforms assess a child's capacity to consent?
- ➔ How will children in care—or those without access to formal guardianship—be supported in exercising their digital rights?
- ➔ Will the Code recommend or require youth-informed formats for presenting consent terms and privacy notices?

The Code must include inclusive, flexible mechanisms for verifying and obtaining consent that reflect the diverse lived realities of Indigenous children. No child should be denied access to safe, rights-respecting digital spaces because of bureaucratic, colonial, or inaccessible consent frameworks.

Privacy Notices and Communication

Plain language is important, but so too is respectful language—especially around concepts such as "ownership," "custody," and "control" of data. These are not neutral terms for Indigenous Peoples; they are legally and politically charged, rooted in sovereignty and self-determination. We'd urge the OPC to reflect critically on the terminology commonly used in privacy and

consent frameworks. While often accepted in mainstream legal and technical contexts, these terms are in tension with Indigenous data sovereignty principles, which emphasize relational responsibility, collective governance, and nation-based rights. For Indigenous children, the framing of data is inseparable from identity, kinship, and cultural continuity, and consent frameworks must be responsive to those deeper meanings.

Privacy notices must do more than meet compliance requirements—they should affirm and uphold children's rights. They must be designed to empower, not overwhelm, young users with clear and accessible information about how their data is collected, used, and shared. This includes mandatory disclosure of AI use, transparent explanations of how automated decisions are made, and the provision of information in formats that are accessible to youth, such as audio-visual tools. Beyond technical clarity, privacy notices should help children understand the broader context of data power, historical misuse, and accountability, equipping them to make informed decisions rooted in both individual and collective awareness.

Sensitive Data Classification

We recommend strong provisions that prohibit the scraping, profiling, or commodification of cultural and community-based data. Indigenous children should never be treated as datasets or algorithmic inputs without free, prior, and informed consent of both individual and collective rights holders. With that we would pose the following questions for the OPC's consideration:

- ➔ Will the Code recognize Indigenous identity and cultural data as sensitive data?
- ➔ How will it support enforcement against misuse by adtech, facial recognition systems, or government surveillance?

Privacy & Digital Literacy Education for Children

Finally, the Code must promote privacy education and digital literacy that is systemic, inclusive, and community-led. Indigenous youth are not only users of technology—they are storykeepers, language learners, organizers, and cultural leaders.

The OPC should actively partner with youth, Indigenous Nations, community-led organizations, schools, and child wellbeing agencies to co-develop privacy education that is culturally grounded and community-defined. This education must go beyond basic safety messaging to build deep data literacy rooted in collective rights, historical context, and self-determination. Indigenous youth deserve tools that help them understand not only how to protect themselves online, but how data systems have impacted their communities and how they can assert their rights within those systems. To ensure this work is meaningful and sustainable, dedicated funding must be made available to Indigenous communities and social services to lead these efforts.

Conclusion

If the Children's Privacy Code is to uphold the rights of all children in Canada, it must intentionally address the digital realities of Indigenous youth and engage with Indigenous Nations as rights holders—not just stakeholders. The harms of colonial data systems cannot be remedied by surface-level reforms or technocratic compliance. What is required is deep listening, principled collaboration, and a refusal to perpetuate the status quo.

We encourage the OPC to take bold steps in aligning this Code with not only Canadian privacy law, but with the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP), the Convention on the Rights of the Child, the Truth and Reconciliation Commission Calls to Action, and the Missing and Murdered Indigenous Women and Girls National Inquiry's Calls to Justice.

We thank you for your time, and we remain available for further dialogue or collaboration.

Sincerely,

Chelsea Nakogee
Co-Founder, Wabusk Data Solutions
chelsea@wabuskdata.ca

Savion Nakogee
Co-Founder, Wabusk Data Solutions
savion@wabuskdata.ca